El tratamiento de imágenes personales en espectáculos deportivos.

Normativa en Chile y estudio de casos extranjeros

Autor

Marcela Cáceres L.
mcaceres@bcn.cl
(56) 32 226 3934

Pedro S. Guerra A.
pguerra@bcn.cl
(56) 32 226 3903

Nº SUP: 140919

Resumen

El documento ofrece una perspectiva actual de la situación de la protección de datos que rige para la obtención de imágenes faciales en el contexto de los espectáculos deportivos. Si bien esta cuenta con una habilitación legal en la ley de violencia en los estadios, Ley N° 19.327, el régimen legal aplicable es el de la Ley N°19.628 sobre protección de la vida privada. Asimismo, la legislación comparada ofrece los siguientes hallazgos:

Colombia ha avanzado en la instalación de un sistema de validación que permita la interoperabilidad para realizar la verificación de identidad para cumplir las sanciones de prohibición de ingreso a estadios. No obstante, los actores que traten información así obtenida, deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio.

En **España** la Ley de Protección de Datos Personales y garantía de los Derechos Digitales de España, adapta el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, que prohíbe tratar datos que revelen datos biométricos para identificar de manera unívoca a una persona física. Los responsables y encargados del tratamiento estarán sujetos al deber de confidencialidad.

En **Dinamarca**, el uso de la tecnología de reconocimiento facial automatizado cuenta con la aprobación previa de la Agencia de Protección de Datos de Dinamarca (DPA). Su objetivo es identificar a las personas a las que se ha prohibido asistir a los partidos de fútbol del equipo por haber infringido las normas de conducta del propio club. Los asesores de protección de datos, designados de conformidad con el reglamento de protección de datos, no deberán transmitir ni utilizar indebidamente información de la que hayan tenido conocimiento en el ejercicio de sus funciones.

Introducción

El presente documento busca responder una solicitud de la Comisión de Deportes y Recreación de la Cámara de Diputadas y Diputados, indagando en los problemas que representa el tratamiento de los datos personales que se obtienen por medio de las tecnologías de reconocimiento facial, en el ámbito de los espectáculos deportivos. Si bien dichas tecnologías se encuentran muy desarrolladas, los marcos normativos vigentes en la actualidad no han seguido el mismo ritmo de avance. En ese sentido, el problema del uso de dichas tecnologías es uno que, jurídicamente, se centra en la captación, almacenamiento y uso de datos personales, y las problemáticas que pueden surgir a partir de estrategias de regulación que equilibren las políticas de seguridad y la adecuada protección de información personal. Asimismo, se examina la forma como se ha implementado en otros países el reconocimiento facial de los hinchas en los estadios, considerando el problema de protección de datos personales que esto implica.

En ese sentido, el documento se organiza de la manera siguiente. Una **primera parte** aborda conceptualmente el reconocimiento facial en tanto tecnología de seguridad pública y privada que impacta en derechos y garantías fundamentales. Una **segunda sección** examina el estado de la cuestión en Chile, identificando el marco legal que le es aplicable al problema en la actualidad y el tratamiento que ofrece el proyecto de ley de protección de datos personales, actualmente en avanzado estado de tramitación en el Senado. Finalmente, la **tercera parte** ofrece un panorama de legislaciones extranjeras que han abordado normativamente el tratamiento de esta clase de datos cuando son obtenidos en el contexto de eventos deportivos y/o futbolísticos. Para este fin, se ha tomado como ejemplo los casos de Colombia, Dinamarca y España, los que no cuentan con una legislación específica sobre reconocimiento facial, pero que, al menos en el caso de los dos países europeos, vistos aplican el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos.

I. ¿Qué es el reconocimiento facial?

El reconocimiento facial es un proceso técnico que se desarrolla mediante tecnologías muy comunes en la vida diaria, que están presentes en sistema de controles de acceso, documentos de identidad como pasaportes o cédulas de identidad y en aplicaciones de telefonía móvil. Esa misma tecnología y sus derivaciones sirven de apoyo en estrategias de seguridad pública, pues permite la identificación de personas de interés, prófugos, personas desaparecidas o delincuentes.

En general los sistemas funcionan a partir de un algoritmo que codifica automáticamente la imagen facial y la compara con perfiles que están almacenados en el sistema o base de información[1]. Esta imagen puede tener su origen en una foto, un video previo o ser captada en tiempo real[2]. El reconocimiento

[1] INTERPOL, 2020.
[2] Para una historia del desarrollo de las técnicas en el campo de la biométrica, véase la entrada sobre el particular en Wikipedia (http://bcn.cl/3ib2u)

facial permite la identificación automática de un individuo detectando y midiendo varias características faciales que se extraen de una imagen y se compara con una base de datos existente. Requiere, en ese sentido, de una recolección de imagen en dos momentos. En una primera ronda, esa imagen es captada y registrada; en una segunda, esa imagen es vuelta a captar y se compara con la plantilla inicial, a partir de la cual se produce la identificación.

Es interesante apuntar que, en el actual estadio de desarrollo de las tecnologías, estas permiten ir bastante más allá de la sola identificación mediante la confrontación de una imagen con una plantilla. Las mediciones biométricas pueden ser de orden fisiológico, codificando ciertas características físicas individuales (huella, forma de las manos, iris, forma de la cara o de las orejas, entre muchos otros); o pueden detectar un comportamiento humano, reconociendo la voz, la dinámica de la firma o la presión y velocidad de la pulsación en un teclado, que van a variar de individuo a individuo de acuerdo al estado físico, la edad, o clase social[3].

Como señala la Agencia Europea de Derechos Fundamentales (*Fundamental Rights Agency*, FRA, por sus siglas en inglés), la investigación en el área permite inferir otras características o estados personales de los sujetos que se someten a ella, como por ejemplo orientación sexual, estados de ánimo o emociones, en procedimientos experimentales que son controversiales desde una perspectiva ética[4].

Es importante destacar, entonces, que las tecnologías de reconocimiento facial se basan en la captación de una imagen facial sobre la cual se produce la comparación. En ese sentido, como afirma la FRA las imágenes faciales constituyen un dato biométrico que no se puede cambiar ni es fácil de ocultar, además de ser relativamente fácil de captar en comparación con otros datos biométricos, como son las huellas digitales[5]. Un dato biométrico es un dato personal que resulta de un procesamiento tecnológico de alguna característica física, psicológica o de comportamiento de una persona natural, que permite confirmar de manera unívoca su identidad[6]. Dado que esta clase de información identifica o permite identificar a una persona, **constituye un dato personal**, pues detecta características biológicas o psicológicas. Santisteban apunta, entonces, que “las técnicas de reconocimiento facial suponen un tratamiento de datos personales”[7]. Esto, como se verá, es corroborado por las normas europeas sobre la materia y por las legislaciones nacionales que se han dictado. De la misma forma, el Consejo para la Transparencia, CPLT en Chile ha estimado en sus recomendaciones que la imagen del rostro de una persona puede “calificar en Chile de datos personales de carácter sensible (…) al corresponder a información que se refiere a las características físicas de una persona natural”[8].

Una de las distinciones más relevantes que pueden ofrecer estas tecnologías dicen relación con su propósito, pues a partir de este se pueden identificar distintas magnitudes de amenazas a derechos fundamentales. Un primer objetivo de estas tecnologías y de la recopilación de datos personales que inevitablemente entraña, es la **verificación** o **autenticación** de una identidad personal. Este es el

[3] Quintanilla, 2020: 68 – 69.
[4] FRA, 2020.
[5] FRA, 2020.
[6] FRA, 2020.
[7] Santisteban, 2021: 507.
[8] CPLT, 2021: 71.

propósito, por ejemplo, de las cámaras que equipan algunos modelos de teléfonos celulares inteligentes. Estos sistemas de verificación uno - a - uno, comparan la imagen con una plantilla única (la propia imagen del dueño del equipo), y no requiere de un almacenamiento centralizado de la imagen[9]. Aquí el tratamiento se adscribe a la persona específica que ha introducido su imagen en la plantilla, y se consideran en general como menos invasivos de la privacidad[10].

En cambio los sistemas destinados a la **identificación** se caracterizan por comparar una imagen individual con las de muchas otras personas que están almacenadas en una base de datos, de forma de determinar si esa imagen individual está contenida o almacenada en esta[11]. Es aquí, como apunta Santisteban, donde pueden observarse mayores riesgos a los derechos fundamentales, como se verá en el párrafo siguiente. Algunos de estos arrancan del uso no autorizado de imágenes de terceros; otros, de la divulgación de esa información y de los resultados de su procesamiento a terceros, ya sea organismos públicos, privados o personas naturales. Es precisamente ante estos riesgos que los sistemas jurídicos han elaborado respuestas más o menos desarrolladas y/o protectoras de los derechos individuales.

Posibles problemáticas que plantea el reconocimiento facial

Las tecnologías que componen los sistemas de reconocimiento facial automático, impactan de manera directa en una serie de derechos y garantías constitucionales y legales, toda vez que existen una serie de instituciones públicas y privadas que captan masivamente una serie de datos personales de sus usuarios, muchas veces con su voluntad y muchas otras sin esta. Esto resulta relevante dado el número creciente de posibles aplicaciones de las tecnologías a una serie de nuevos ámbitos, y siempre en crecimiento. De ahí que el uso de estas tecnologías y sus dispositivos, ofrece un campo para discusiones jurídicas y políticas que pueden recorrer un espectro más o menos amplio de prohibición o permisividad.

Estos riesgos se originan ya en problemas técnicos que se verifican aún en el actual estado de desarrollo de las tecnologías; y otros que, derivando de estas, constituyen desajustes entre las prácticas que originan las mismas tecnologías y los derechos fundamentales que se contienen en cuerpos normativos constitucionales.

Los riesgos que se generan en **problemas técnicos** de las tecnologías aluden a que, si bien las tasas de error son menores[12], los sistemas son proclives a que ciertas categorías de personas sean identificadas erróneamente con más frecuencia que otras. Dado que las respuesta que proveen son binarias (se identifica o no) los mecanismos son susceptibles a producir falsos (positivos o negativos) en base a un cálculo probabilístico que el sistema mecaniza a alta velocidad. Como indica la FRA esto depende en buena parte de la calidad de la información con que se nutre la base de datos en la que el sistema busca una coincidencia facial. La calidad de las imágenes resulta fundamental, y no siempre es óptima. Asimismo, como destaca la FRA, los *softwares* de reconocimiento facial se basan en modelos

[9] FRA, 2020.
[10] Santisteban, 2021: 507.
[11] FRA, 2020.
[12] FRA indica que el 0.01% de las identificaciones masivas en lugares como estaciones de trenes o aeropuertos, son erróneas. Ello implica, aun, que cientos de personas son erróneamente identificadas (FRA, 2020).

pre – entrenados que desarrollan reglas de identificación basadas en bases de datos con imágenes disponibles. En otras palabras, los sistemas son "enseñados" para desarrollar esa labor de identificación en base a la mayor o menor cantidad de información disponible y a un poder de computación dado y creciente. En estas condiciones, la falibilidad/fiabilidad del sistema descansa necesariamente en la calidad y la cantidad de información de que dispone para su labor; pero su entrenamiento en sí, es decir la determinación de la forma en que operará, no está libre de sesgos. Como reporta la FRA los sistemas de reconocimiento facial reportan problemas en identificación en género y grupos étnicos

> "(…) debido a que el *software* de reconocimiento facial es a menudo entrenado principalmente sobre imágenes faciales de hombres blancos y, en mucha menor medida, de mujeres y personas pertenecientes a otros grupos étnicos."[13]

Desde la perspectiva **jurídico – política**, como se evidencia en las discusiones de literatura, los dilemas radican en la mayor o menor afectación que las estrategias de seguridad basadas en el uso de la video vigilancia, y específicamente del reconocimiento facial automático, pueden generar para los derechos fundamentales. Ello a partir de la posición desmejorada o de debilidad de las personas cuyos rostros son captados y chequeados por los sistemas de vigilancia[14].

Pérez identifica los problemas más gruesos en torno al derecho al derecho a la igualdad y la no discriminación; la garantía de presunción de inocencia; y el derecho a la privacidad[15]. Este último, para Santisteban, constituye un presupuesto para el ejercicio de otros derechos, como la libertad de expresión, pues este último reclama de cierto anonimato en el espacio público[16]. Como se advierte, el espectro de derechos que pueden afectarse en el uso de tecnologías de esta clase es amplio, y dependerá de la robustez de las estructuras de protección existentes en cada nación y de la *accountability* pública de instituciones privadas y del Estado. No es posible, en consecuencia, ofrecer un análisis exhaustivo, pues nuevas formas de afectación pueden aparecer en circunstancias específicas.

No obstante, como se señalaba y siguiendo a la FRA[17], hay un *set* de derechos que debe tenerse en consideración en el desarrollo e implementación básicos de una regulación. El primer grupo lo componen el respeto a la vida privada y la protección de los datos personales. El derecho a la protección puede considerarse una extensión del primero, pero ambos emanan de la dignidad y la autonomía de la persona humana, que granjea una esfera personal en que se impide a otros la intromisión. El segundo grupo lo componen las libertades de expresión, reunión y asociación.

II- El estado de la cuestión en Chile

El presente acápite aborda el estado de la cuestión en Chile, identificando la normativa que actualmente se aplica a la recolección y tratamiento de datos personales. Finalmente, se muestran algunos rasgos

[13] FRA, 2020.
[14] FRA, 2020.
[15] Pérez, 2022:54.
[16] Santisteban, 20221: 505.
[17] FRA, 2020.

del proyecto de ley de protección de datos personales, actualmente en tramitación en el Senado[18] y que incide directamente en el problema.

Normativa vigente

Como se ha señalado en otros documentos de Asesoría Técnica Parlamentaria de la Biblioteca del Congreso Nacional[19], el principal texto legislativo sobre protección de datos personales en Chile es la **Ley N°19.628 sobre protección de la vida privada**[20]. Como se advierte, esta regulación se sitúa en el marco de la protección de la vida privada y de los datos personales, garantizado en la Constitución Política de la República (artículo 19, N°4). La garantía de protección de los datos personales, de acuerdo con la norma, se remite a la ley, que establecerá la forma y condiciones de protección de esos datos.

En ese sentido, el artículo 2, letra f) de la Ley N°19.628 define los datos de carácter personal como "(…) los relativos a cualquier información concerniente a personas naturales, identificadas o identificables." Una clase específica de datos personales son los datos sensibles, que define el mismo artículo en su letra g). Se trata de

> "(…) aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual."

Desde esta perspectiva, y según las definiciones del punto I de este documento, las imágenes de rostros de las personas, y por cierto las de los asistentes a un evento deportivo, son posibles de considerar como **dato personal sensible**, de acuerdo a la actual legislación. Este concepto debe entenderse de manera complementaria con la de tratamiento de datos que se define en el artículo 2, letra o) como

> "(…) cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma."

De este modo, los sistemas de reconocimiento facial, como han sido descritos antes, corresponden a un sistema de tratamiento de datos, al menos en una considerable extensión del concepto que ofrece la ley chilena.

Esta idea de tratamiento de datos va a ser fundamental para comprender la dimensión normativa actual del reconocimiento de rostros. Ello a partir del artículo 4 de la Ley N°19.628, que ordena que el tratamiento de datos sólo puede efectuarse cuando la ley u otras disposiciones legales lo autoricen; o bien cuando el titular de los derechos consienta expresamente en ese tratamiento. Teniendo en cuenta

[18] Proyecto de ley que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales (Boletín 11092-07 y 11144-07, refundidos). Disponibles en http://bcn.cl/3iatc
[19] BCN, 2023; BCN, 2014.
[20] Disponible en https://bcn.cl/2f7cg

esas restricciones, y la regulación detallada que la ley hace de la forma de otorgar ese consentimiento[21], es preciso determinar si la ley chilena autorizaría el tratamiento de imágenes personales que hayan sido captadas por sistema de reconocimiento facial.

La primera consideración que debe hacerse es que, como señala el Consejo para la Transparencia (CPLT)[22], la tecnología de reconocimiento facial no posee una regulación expresa en la legislación. Eso hace aplicable el régimen general de la Ley N°19.628, en su acápite de datos personales. Entonces, una entidad que opera en Chile un sistema de video - vigilancia o de reconocimiento facial, está obligada a cumplir con las normas de esta ley. Estas obligaciones legales le incumben a cualquier persona natural o jurídica que opere el sistema en calidad de responsable de banco de datos, ya sean instituciones públicas o privadas. En ese sentido, para el CPLT es claro que el funcionamiento de los sistemas de videovigilancia y captación de imágenes implica necesariamente el tratamiento de datos personales en los términos en los que lo define la ley e independientemente del nivel de cada operación[23]. Esto incluye, en cualquier caso

> "(…) el match realizado entre los datos captados mediante cámaras con una base de datos que contenga datos biométricos o huellas faciales y que fueron almacenados con anterioridad."[24]

Es importante destacar que, si bien la ley no contempla actualmente una mención que defina los datos biométricos, como han sido caracterizados antes en este documento, lo cierto es que estos bien pueden considerarse como parte de la categoría general de datos personales sensibles. Este es un criterio que ya ha sido adoptado por el Consejo para la Transparencia en Chile, y que replica por lo demás las normas sobre el particular que se contienen en la normativa europea.

Asimismo, el alcance la regulación actual para el problema del tratamiento de imágenes faciales, es también amplio, y comprende tanto las imágenes que se obtienen del rostro de una persona como aquellas que ya se encuentran almacenadas en otras bases y que van a servir para la comparación e identificación de una persona. Estas últimas suelen denominarse "*watch list*" o lista de vigilancia, y se compilan por las policías y fuerzas de seguridad, para después ser sometidas al cotejo digital.

La aplicación del régimen de la Ley Nº19.628 a los datos personales sensibles que constituyen las imágenes faciales impone al tratamiento de dichas imágenes algunos requisitos. Debe, en primer lugar, estar expresamente contenido en una ley; en caso de no estarlo, debe resultar imprescindible para el debido cumplimiento de una función pública establecida por ley, en caso de que el tratamiento corresponda a organismos públicos en ejercicio de una función que les es propia (artículo 20 de la Ley Nº19.628). En segundo lugar, debe haber sido obtenida con el consentimiento del titular, expreso, por escrito y previa información a este.

---

[21] Según el mismo artículo 4, el consentimiento debe otorgarse por escrito y previa información al titular. La excepción al consentimiento es el caso de datos que provienen de fuentes accesibles al público.
[22] CPLT, 2021: 69.
[23] CPLT, 2021: 72.
[24] CPLT, 2021: 72.

Como se advierte, la base de legalidad para el tratamiento de las imágenes personales o faciales captadas por sistemas de reconocimiento es, en la actualidad, la ley o el consentimiento del titular. Dadas las condiciones de operación en que se captan imágenes faciales de personas, por ejemplo en el acceso a un estadio para presenciar un espectáculo deportivo, estas no contarían con un respaldo de legalidad en la actual normativa que rige en Chile, y su tratamiento, en el más amplio sentido, no estaría autorizado por la ley. Ello salvo que las personas que son captadas otorguen su consentimiento, en los términos que dispone la Ley Nº 19.628.

El caso de los espectáculos deportivos

No obstante lo que se ha dicho, y a objeto de acotar el problema a los espectáculos deportivos futbolísticos, es preciso considerar las normas que contiene al respecto la Ley Nº 19.327[25] sobre derechos y deberes en los espectáculos de futbol profesional. En general, el artículo 3 dispone la obligación de los organizadores de este tipo de eventos de adoptar medidas de seguridad que disponga la autoridad para prevenir alteraciones a la seguridad y el orden público producto de la realización de un espectáculo de futbol profesional. Este deber se complementa con obligaciones específicas que se contienen en el artículo 5º. En especial la letra g)[26] dispone el deber de

> "Disponer de medios de grabación, a través de cámaras de seguridad, que tengan los estándares de calidad suficientes para identificar a los asistentes al espectáculo de fútbol profesional, junto con vigilar el perímetro del lugar donde se celebre el mismo. Estas cámaras deberán ser monitoreadas permanentemente por los organizadores durante el desarrollo del espectáculo, debiendo resguardarse sus imágenes por un período mínimo de noventa días, sin perjuicio de lo señalado en el artículo 3º bis."

Esta norma ofrece una contradicción aparente con las normas de protección de datos sensibles, que se han referido anteriormente. En efecto, esta norma obliga al organizador a disponer de un medio de grabación con la precisa y concreta finalidad de identificar a los asistentes a un espectáculo de futbol profesional en el estadio y su perímetro. Además, dispone de normas muy básicas para su tratamiento, obligando a su resguardo por un mínimo de 90 días.

Sin embargo, las normas de la Ley N°19.327 deben comprenderse de manera complementaria con las de la Ley de Protección de la Vida Privada, N° 19.628. En efecto, la Ley de violencia en los estadios equivale a una habilitación legal suficiente para permitir, por parte de una entidad privada, la captación de esas imágenes faciales de los asistentes. Dado que la norma de la Ley Nº 19.327 no dispone un régimen para el manejo de esos datos (más allá de establecer un plazo mínimo para su conservación) ese régimen vendría dado por las normas de la Ley Nº19.628, con todos los defectos y virtudes que esta puede tener. En ese sentido, el estándar que debe cumplir la captación de imágenes por los sistemas de seguridad de los estadios de futbol viene determinado por las normas de protección de datos hoy vigentes, y que se contienen en la Ley Nº19.628. Ello debido a que la Ley N°19.327 no contiene, propiamente, un régimen de tratamiento de esos datos. Finalmente, debe recordarse que el ámbito de esta última ley está acotado a los espectáculos de futbol.

---

[25] Disponible en https://bcn.cl/3858z

[26] Esta norma fue introducida como se lee por la Ley Nº20.844 de 2015, que modificó en varias partes a la Ley Nº 19.327.

Proyecto de ley sobre protección de datos personales

Como es sabido, se encuentra actualmente en tercer trámite constitucional en el Senado el proyecto de ley de protección de datos personales[27] que reforma la Ley N°19.628, y que incide directamente en el problema que se ha tratado en este documento. En lo sucesivo se examinan algunos aspectos de dicho proyecto que pueden resultar interesantes para desarrollar una perspectiva regulatoria sobre los sistemas de reconocimiento facial en el futuro.

Es preciso destacar que este proyecto obedece en buena parte a las críticas que ha recibido el actual sistema de protección de datos personales. En ese sentido, el Consejo para la Transparencia ha señalado que la actual legislación resulta insuficiente para el objetivo de protección. Entre otras críticas, destaca que los principios de tratamiento de los datos están regulados de forma inorgánica y deficiente, que las bases de legalidad son limitadas, pues de basan únicamente en la ley y el consentimiento del titular, y que no se contemplan regulaciones sobre categorías de datos relevantes, como los datos biométricos y de geolocalización. El corolario es que no existe "un mayor control respecto de la implementación en Chile de tecnologías de videovigilancia y reconocimiento facial, por ejemplo, en contextos de seguridad de espacios públicos."[28].

En ese orden, el proyecto de ley innova en los siguientes aspectos relativos a la protección de esta clase de datos.

1. **Definición de dato personal**: el proyecto contempla definirlos como

> "(…) cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona**,** excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado."

2. **Definición datos personales sensibles**: la modificación propuesta, actualmente en discusión, es la siguiente

> "(…) sólo tendrán esta condición aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, hábitos personales, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural."

---

[27] Proyecto de ley que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales (Boletín 11.092-07 y 11.144-07, refundidos). El examen que aquí se ofrece se basa en la última versión del proyecto de ley, al 04 de enero de 2024. Disponible en http://bcn.cl/2ei1m

[28] CPLT, 2021: 85 – 86.

3. **Definición de dato biométrico:** el proyecto de ley, a diferencia de la ley actual, sí ofrece un concepto de dato biométrico, como

> (…) aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de ella, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz.

Como se advierte, las definiciones que propone el proyecto de ley permiten incorporar categorías más amplias de lo puede comprenderse como dato personal sensible, en los que queda claramente incorporado. Esto se debe comprender como parte de un conjunto de definiciones que componen el sistema de protección, como la de "elaboración de perfiles" (formas de tratamiento automatizado de datos personales para análisis o predicción) o "tratamiento de datos" (cualquier operación o procedimientos técnicos, que permitan utilizar de cualquier forma datos o conjuntos de datos personales).

En un mismo sentido, una de las innovaciones del proyecto en relación a la actual ley, es el establecimiento de principios que gobiernan el uso protegido de los datos. Entre los más relevantes, y que inciden directamente en la cuestión de la identificación facial por sistemas de televigilancia, están el **principio de licitud,** que implica que los datos personales sólo pueden tratarse con sujeción a la ley; y el de **finalidad,** que exige que los datos sean recolectados con fines específicos, explícitos y lícitos, y que su tratamiento esté limitado a esos fines.

III. Regulación de mecanismos de reconocimiento facial de hinchas en estadios deportivos en Colombia, España y Dinamarca

1. Colombia

El 5 de Agosto del año 2022, el Gobierno del Presidente Iván Duque, expidió el **Decreto N° 1.622**[29], por medio del cual se adiciona la Parte 17 del Libro 2 del Decreto 1085 de 2015, Decreto Único Reglamentario del Sector Administrativo del Deporte, en lo relacionado con la regulación del ingreso a los eventos de fútbol profesional como medida para garantizar la seguridad y convivencia en los estadios.

Su objetivo es establecer mecanismos de seguridad para la convivencia en el fútbol profesional, implementando por etapas la reglamentación en la venta, emisión de la boletería y el sistema de ingreso de aficionados a los eventos de fútbol profesional en Colombia.

En un comienzo, la legislación busca estandarizar el proceso de adquisición y emisión de boletas, así como el ingreso a los estadios de fútbol en Colombia, mediante la asociación de la boleta al documento

[29] Disponible en http://bcn.cl/3id7u

de identidad, que permita la verificación, previa a su adquisición, de antecedentes de los espectadores para hacer efectivas las restricciones de derecho de admisión en los eventos futbolísticos que se encuentran estipulados en la legislación vigente[30].

No obstante, posteriormente señala que "toda la información de los usuarios que se genere, almacene, transmita o trate en el marco de la venta, emisión de la boletería y el sistema de ingreso de aficionados, deberá ser protegida y custodiada bajo los más estrictos esquemas de seguridad digital y privacidad con miras a garantizar la autenticidad, integridad, disponibilidad, confidencialidad, el acceso y circulación restringida de la información, de conformidad con lo estipulado en la Ley N°1.581 de 2012"[31] .

Más aún, plantea la implementación de un **Sistema de Validación Nacional**, o sea un desarrollo tecnológico o *software*, que permitirá la interoperabilidad para realizar la verificación de las sanciones vigentes de prohibición de ingreso a escenarios deportivos. Además, permitirá efectuar la validación de la identidad, verificación de medidas de aseguramiento y requerimientos judiciales, de acuerdo con el artículo 2.17.7 de la Ley N°1.581 de 2012[32].

Este sistema será administrado y operado por el Gobierno nacional, a través del Ministerio del Deporte, quien podrá delegar en un tercero su creación, manutención, actualización y operación.

El operador del Sistema de Validación Nacional y los comercializadores de boletería serán responsables en lo que les corresponda, del tratamiento de los datos personales que los ciudadanos le suministren directamente. Asimismo, serán los encargados del tratamiento de los datos que otras entidades les proporcionen, según dispone el artículo 2.17.12[33]. Los operadores de los datos quedan obligados en los términos del artículo 2.17.13:

> "Los actores que traten información en el marco de la presente parte deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, en la cual deberán hacer periódicamente una evaluación del riesgo de seguridad digital que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo".

El Sistema de Validación Nacional tendrá tres fases y luego de su completo funcionamiento, el Ministerio del Deporte evaluará la posibilidad de implementar la tecnología de reconocimiento por biometría facial para el ingreso a los eventos de fútbol profesional. El Ministerio del Deporte, en un plazo razonable, podrá expedir el procedimiento a través del cual se adoptaría este mecanismo y se integraría al Sistema de Validación Nacional, según el artículo 2.17.22.[34].

[30] Presidencia de la República de Colombia, 2022.
[31] Disponible en http://bcn.cl/3id7z
[32] Presidencia de la República de Colombia, 2022.
[33] Presidencia de la República de Colombia, 2022.
[34] Presidencia de la República de Colombia, 2022.

2. España

En España el reconocimiento facial avanza como un procedimiento de entrada a los recintos deportivos. La **Ley de Protección de Datos Personales y garantía de los Derechos Digitales**[35], adapta el ordenamiento jurídico español al **Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas**[36] en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos. El reglamento europeo prohíbe expresamente en su artículo 6, N°1.

> "tratar datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas, el tratamiento de datos genéticos, **datos biométricos** para identificar de manera unívoca a una persona física, de salud, o relativos a la vida y orientación sexual de una persona". *Énfasis nuestro.*

De acuerdo con la misma norma, el texto europeo establece algunos límites al tratamiento, entre ellos que el interesado otorgue un consentimiento explícito, para proteger intereses vitales del interesado o de otra persona física, que sea estrictamente necesario por razones de un interés público esencial[37] o en el ejercicio de poderes públicos conferidos al responsable. Ello de acuerdo con el artículo 8, N°2 de la Ley de Protección de Datos Personales y garantía de los derechos digitales[38].

La ley española, entiende por **consentimiento** del afectado

> "toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

Asimismo, el consentimiento del afectado puede ser otorgado para uno o varios objetivos por lo que "cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas".

Respecto del **tratamiento necesario por razones de un interés público esencial** fundados en el derecho español, deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

El artículo 5 de la Ley española dispone que los responsables y encargados del tratamiento estarán sujetos al deber de confidencialidad y deberán designar un delegado de protección de datos[39], y cuando se trate de entidades entre las que se cuentan las federaciones deportivas en la medida que gestionen

---

[35] Disponible en http://bcn.cl/3id8b
[36] Disponible en http://bcn.cl/3id86
[37] Artículo 6, N°1.
[38] Artículo 8, N°2.
39 La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

datos de menores de edad (artículos 31 a 37). De este modo, entre las obligaciones se disponen las siguientes:

- Nombrar un responsable proactivo con conocimiento especializado en derecho y en la práctica de protección de datos.

- Establecer un registro de actividades de tratamiento: se podrá constituir sobre la base de las informaciones de los ficheros de tratamientos notificados al Registro General de Protección de Datos de la Agencia.

- Realizar análisis de riesgos y medidas de seguridad: los riesgos varían según los tipos de tratamiento, la naturaleza de los datos, el número de afectados y la cantidad y variedad de tratamientos. Los riesgos no son estáticos por lo que corresponderá al responsable, luego de determinarlos, establecer las medidas de seguridad necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales

- Evaluar el impacto en la protección de datos. Esta se comprende como una "herramienta de carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas física."[40].

- Evaluación sistemática y exhaustiva de aspectos personales de personas naturales que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.

- Tratamiento a gran escala de las categorías especiales de dato, como los biométricos (imágenes). En este caso, para determinar si es de "gran escala" se debe considerar: número de interesados afectados, bien como cifra o como proporción de la población correspondiente; el volumen de datos o la variedad de elementos de datos distintos que se procesan; la duración, o permanencia de la actividad de tratamiento de datos y alcance geográfico de la actividad de tratamiento. El Reglamento determina los supuestos en que debe realizarse una evaluación de impacto.

- Observación sistemática a gran escala de una zona de acceso público.

- Tener en cuenta la privacidad desde el diseño y por defecto. Éste incluye dos principios:

  - Principio de protección de datos desde el diseño supone que la protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo.

[40] BCN, 2019.

- Principio de protección de datos por defecto supone, de acuerdo con el artículo 25 del reglamento, que se adopten las medidas técnicas y organizativas apropiadas para garantizar que por defecto, sólo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento[41].

Asimismo, disposición final undécima la ley española en su modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[42], señala en su N°2, del apartado 1 del artículo 15, párrafo 2 que,

> "Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o **biométricos** o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley". *Énfasis nuestro.*

En caso de posible vulneración de la normativa de protección de datos**,** la Ley 3/2018 dispone que corresponderá a la

> "Presidencia de la Agencia Española de Protección de Datos cuando proceda, dictar un acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción". [43].

Por su parte el artículo 68 señala que "cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo"[44].

El régimen sancionador establecido en el Reglamento (UE) 2016/679 y en el artículo 70 de la Ley de Protección de Datos, se aplica a los responsables, encargados, representantes de los responsables o encargados de los tratamientos, entidades de certificación y aquellas acreditadas de supervisión de los códigos de conducta. No obstante, no será de aplicación al delegado de protección de datos.

Con respecto a los sistemas de reconocimiento de imágenes en los partidos de futbol profesional, cabe señalar que a comienzos de este 2024, la Agencia Española de Protección de Datos hizo una advertencia a La Liga de fútbol ante la licitación de un contrato para desarrollar un sistema de reconocimiento facial para el acceso de los aficionados a los estadios. La razón, la necesidad de que un

---

[41] Artículo 25.
[42] Disponible en http://bcn.cl/3idds
[43] La Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier Convenio Internacional en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos. Artículo 56, N°2.
[44] Artículo 68.

sistema de este tipo se ajustase a la legalidad y que en caso de no adoptar las medidas necesarias incurriría en una infracción[45].

La agencia ha instado a La Liga a verificar si puede producirse alguno de los supuestos previstos en el Reglamento General de Protección de Datos, de modo que no sea de aplicación la prohibición general del tratamiento de los datos personales[46].

3. Dinamarca

En 2019, el equipo de fútbol danés Brøndby IF anunció que a partir de julio de ese año implementaría la tecnología de reconocimiento facial automatizado (*Automated Facial Recognition*, AFR, por sus siglas en inglés) en su estadio.

En Dinamarca, el uso de esta tecnología cuenta con la aprobación previa de la Agencia de Protección de Datos de Dinamarca (DPA). Su objetivo es identificar a las personas a las que se ha prohibido asistir a los partidos de fútbol del equipo por haber infringido las normas de conducta del propio club en partidos anteriores.

El sistema funciona mediante cámaras que escanean la zona del público situada frente a las entradas del estadio, de modo que las personas que figuren en la lista de prohibidos puedan ser identificadas entre la multitud antes de llegar a la entrada[47].

La Ley de disposiciones complementarias al reglamento sobre la protección de las personas físicas en relación con el tratamiento de datos personales y sobre el libre intercambio de dicha información (Ley de Protección de Datos, complementa y aplica el Reglamento Nº 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en relación con el tratamiento de datos personales y al libre intercambio de dicha información[48].

Como se señaló anteriormente en el caso de España, el artículo 9 del Reglamento General de Protección de Datos prohíbe el tratamiento de datos personales sensibles, como los datos biométricos generados por el reconocimiento facial automatizado, con el fin de identificar de manera unívoca a una persona, salvo que se aplique una de las condiciones especificadas en el artículo 9, apartado 2. El consentimiento explícito del interesado es una de estas condiciones. Sin embargo, el consentimiento no puede ser la base jurídica para utilizar el AFR, ya que el consentimiento debe ser voluntario, de acuerdo con el Reglamento.

Basándose en el artículo 9, apartado 2, letra g), las disposiciones complementarias danesas del Reglamento General de Protección de Datos contienen una excepción general a la prohibición de tratar datos personales sensibles. El artículo 7(4) de la Ley de Protección de Datos establece que "el tratamiento de datos cubiertos por el artículo 9(1) del Reglamento General de Protección de Datos,

[45] Agencia Española de Protección de Datos, 2024.
[46] Moya, 2024.
[47] Bora, 2021.
[48] Danish Parliament, 2018.

puede tener lugar si el tratamiento es necesario por razones de interés público sustancial"[49] (Danish Parliament, 2018). Se requiere autorización previa de la ADP para los responsables del tratamiento que no sean autoridades públicas, y esta autorización puede establecer condiciones más detalladas para el tratamiento.

La información cubierta por el reglamento de protección de datos, artículo 9, inciso 1 podrá procesarse si se hace únicamente con el propósito de ejecutar sistemas de información legal de importancia social significativa, y si el procesamiento es necesario para el funcionamiento de los sistemas. La información, no podrá ser procesada para otro fin[50]. En todo caso, la autoridad de control podrá anunciar condiciones adicionales para los tratamientos mencionados en el inciso 1.

De acuerdo con el artículo 37, la información regulada por la presente ley puede transferirse para su almacenamiento en un archivo de conformidad con las normas de la legislación sobre archivos[51]. Asimismo, los asesores de protección de datos designados de conformidad con el reglamento de protección de datos, no deberán transmitir ni utilizar indebidamente información de la que hayan tenido conocimiento en el ejercicio de sus funciones como asesores en protección de datos.

Cualquier persona que haya sufrido un daño material o inmaterial como resultado de una actividad de procesamiento ilegal o de cualquier otro procesamiento contrario a esta ley y al reglamento de protección de datos, tiene derecho a una indemnización[52] (Danish Parliament, 2018).

La asociación *European Digital Rights* (EDRi) ha advertido de que la decisión de la DPA danesa,

> "es bastante difícil de entender en el presente caso. El reconocimiento facial automatizado es una de las tecnologías de vigilancia más invasivas, ya que permite identificar a un gran número de personas en una multitud a partir de sus datos biométricos (imágenes faciales) y catalogarlas automáticamente basándose en coincidencias con listas de vigilancia predefinidas. Al mismo tiempo, el AFR es una tecnología muy poco fiable e inexacta, con sesgos sistemáticos conocidos en forma de tasas de error más elevadas para determinadas minorías étnicas"[53].

Según EDRi, la autorización de la DPA no menciona la exactitud del AFR, y no hay requisitos específicos para que el responsable del tratamiento tome medidas para limitar las identificaciones falsas positivas o incluso hacer un seguimiento de la magnitud de este problema[54].

[49] Danish Parliament, 2018.
[50] Artículo 9. Inciso 1 y 2.
[51] Artículo 14.
[52] Artículo 40.
[53] Bora, 2021.
[54] Lund, 2019.

Referencias Generales

Agencia Española de Protección de Datos. (11 de Enero de 2024). *La Agencia Española de Protección de Datos avisa a La Liga por los sistemas de reconocimiento facial en estadios*. España. Recuperado el 13 de Marzo de 2024, de https://efe.com/deportes/2024-01-11/proteccion-de-datos-advierte-liga-sobre-sistemas-reconocimiento-facial-estadios/

BCN, 2019. *Tratamiento de imágenes de video vigilancia. Legislación comparada, guías y recomendaciones*. España. Recuperado el 14 de Marzo de 2024, de https://www.bcn.cl/asesoriasparlamentarias/detalle_documento.html?id=74619

BCN, 2023: Protección de datos relativos a la salud: régimen sancionatorio en la legislación nacional. Disponible en http://bcn.cl/3ibsr

BCN, 2014: Régimen legal nacional de la protección de datos personales. Disponible en http://bcn.cl/2y406

Bora. (2021). *The Use of Automated Facial Recognition in Football Across Europe*. Recuperado el 15 de Marzo de 2024, de https://welcometobora.com/blog/privacy-rights-groups-warn-against-the-use-of-automated-facial-recognition-in-football-fields-across-europe/

Consejo para la Transparencia, CPLT, 2021: La Protección de datos personales en contextos de avanzado desarrollo tecnológico con énfasis en videovigilancia y tecnología de reconocimiento facial empleada por el sector público: noviembre 2021. Disponible en http://bcn.cl/3ic4r

European Union Agency for Fundamental Rights, FRA, 2020: *Facial Recognition technology: fundamental rights considerations in the context of law enforcement.* Disponible en http://bcn.cl/3idfj

Lund, J. (19 de Junio de 2019). *Danish DPA approves Automated Facial Recognition*. Recuperado el 15 de Marzo de 2024, de https://edri.org/our-work/danish-dpa-approves-automated-facial-recognition/

Moya, C. (11 de Enero de 2024). *La Agencia Española de Protección de Datos avisa a La Liga por los sistemas de reconocimiento facial en estadios*. España. Recuperado el 13 de Marzo de 2024, de https://efe.com/deportes/2024-01-11/proteccion-de-datos-advierte-liga-sobre-sistemas-reconocimiento-facial-estadios/

Pérez, N., 2022. *Los sistemas de reconocimiento facial: una mirada a la luz del examen de proporcionalidad*. En Revista Internacional de Derechos Humanos, Vol. 12, N°1.

Quintanilla, G., 2020: *Legislación, riesgos y retos de los sistemas biométricos*. En Revista Chilena de Derecho y Tecnología, Vol. 9, Num. 1, pp. 63 -91.

Santisteban, M., 2021: *Reconocimiento facial y protección de datos: una respuesta provisional a un problema pendiente*. En Revista de Derecho UNED, num. 28. pp. 499 -526.

Senado, 2024: Proyecto de ley que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales (Boletín 11.092-07 y 11.144-07, refundidos). Disponibles en http://bcn.cl/2ei1m

Normativas

Chile

Ley Nº 19.327 de derechos y deberes en los espectáculos de futbol profesional. Disponible en https://bcn.cl/3858z

Ley N°19.628 sobre protección de la vida privada. Disponible en https://bcn.cl/2f7cg

Colombia

Presidencia de la República de Colombia. (5 de Agosto de 2022). *Decreto 1622 de 2022*. Colombia. Recuperado el 15 de Marzo de 2024. Disponible en http://bcn.cl/3id7u

Ley N°1.581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Disponible en http://bcn.cl/3id7z

España

Jefatura del Estado. Ley Orgánica 3/2018 de 5 de diciembre, de protección de datos personales y garantía de derechos digitales. Disponible en http://bcn.cl/3id8b

Jefatura del Estado. Ley 19/2013 de 09 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Disponible en http://bcn.cl/3idds

Parlamento Europeo y Consejo de la Unión Europea (27 de Abril de 2016). Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Unión Europea. Recuperado el 13 de Marzo de 2024, de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Dinamarca

Danish Parliament. (23 de mayo de 2018). *Act N° 502, Data protection Act*. Dinamarca. Recuperado el 15 de Marzo de 2024, de https://www.retsinformation.dk/eli/lta/2018/502